Claims

[c1] A smartcard transaction system configured with a bio-metric security system, said system comprising:

a smartcard configured to communicate with a reader;

a reader configured to communicate with said system;

an iris scan sensor configured to detect a proffered iris scan sample, said iris scan sensor configured to communicate with said system; and,

a device configured to verify said proffered iris scan sample to facilitate a transaction.

[c2] The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

[c3] The smartcard transaction system of claim 1, wherein said iris scan sensor is configured to facilitate a finite number of scans.

[c4] The smartcard transaction system of claim 1, wherein said iris scan sensor is configured to log at least one of a detected iris scan sample, processed iris scan sample and stored iris scan sample.

[c5]   The smartcard transaction system of claim 1, further in-
         cluding a database configured to store at least one data
         packet, wherein said data packet includes at least one of
         proffered and registered iris scan samples, proffered and
         registered user information, terrorist information, and
         criminal information.

[c6]   The smartcard transaction system of claim 4, wherein
         said database is contained in at least one of the smart-
         card, smartcard reader, sensor, remote server, merchant
         server and smartcard system.

[c7]   The smartcard transaction system of claim 5, wherein
         said remote database is configured to be operated by an
         authorized sample receiver.

[c8]   The smartcard transaction system of claim 1, wherein
         said iris scan sensor device is configured with one of a
         video camera, an optical scanner, a digital camera, and a
         charge coupled device.

[c9]   The smartcard transaction system of claim 1, wherein
         said iris scan sensor is configured to detect and verify
         iris scan characteristics including surface patterns.

[c10]   The smartcard transaction system of claim 9, wherein
         said iris scan sensor configured to detect and verify iris

scan characteristics is further configured to localize the boundaries and the eyelid contours of the iris and to create a phase code for the texture sequence of the iris.

[c11]   The smartcard transaction system of claim 1, wherein said iris scan sensor device is configured to detect and verify pupil dilation, eyeball pressure and body heat.

[c12]   The smartcard transaction system of claim 1, further including a device configured to compare a proffered iris scan sample with a stored iris scan sample.

[c13]   The smartcard transaction system of claim 12, wherein said device configured to compare an iris scan sample is at least one of a third-party security vendor device and local CPU.

[c14]   The smartcard transaction system of claim 12, wherein a stored iris scan sample comprises a registered iris scan sample.

[c15]   The smartcard transaction system of claim 14, wherein said registered iris scan sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment informa-

tion and loyalty point information.

[c16] The smartcard transaction system of claim 15, wherein different registered iris scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c17] The smartcard transaction system of claim 15, wherein an iris scan sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein an iris scan sample is secondarily associated with second user information, wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment infor-

mation and loyalty point information, and wherein said second user information is different than said first user information.

[c18]   The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered iris scan sample.

[c19]   The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered iris scan sample.

[c20]   The smartcard transaction system of claim 1, wherein said sensor is configured to provide a notification upon detection of a sample.

[c21]   The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

[c22]   The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

[c23]   A method for facilitating biometric security in a smart-card transaction system comprising: proffering an iris

scan to an iris scan sensor communicating with said system to initiate verification of an iris scan sample for facilitating authorization of a transaction.

[c24] The method for of claim 23, further comprising registering at least one iris scan sample with an authorized sample receiver.

[c25] The method of claim 24, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering an iris scan to said authorized sample receiver, processing said iris scan to obtain an iris scan sample, associating said iris scan sample with user information, verifying said iris scan sample, and storing said iris scan sample upon verification.

[c26] The method of claim 23, wherein said step of proffering includes proffering an iris scan to at least one of a video camera, an optical scanner, a digital camera, and a charge coupled device.

[c27] The method of claim 23, wherein said step of proffering further includes proffering an iris scan to an iris scan sensor communicating with said system to initiate at least one of: storing, comparing, and verifying said iris scan sample.

[c28]   The method of claim 23, wherein said step of proffering an iris scan to an iris scan sensor communicating with said system to initiate verification further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c29]   The method of claim 23, wherein said step of proffering an iris scan to an iris scan sensor communicating with said system to initiate verification further includes comparing a proffered iris scan sample with a stored iris scan sample.

[c30]   The method of claim 29, wherein said step of comparing includes comparing a proffered iris scan sample to a stored iris scan sample by using at least one of a third-party security vendor device and local CPU.

[c31]   The method of claim 29, wherein said step of comparing includes comparing iris scan characteristics including surface patterns.

[c32]   The method of claim 23, wherein said step of proffering an iris scan to an iris scan sensor communicating with said system further comprises using said iris scan sensor to detect at least one of pupil dilation, eyeball pressure

and body heat.

[c33]   The method of claim 23, wherein said step of proffering an iris scan to an iris scan sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered iris scan sample.

[c34]   The method of claim 23, wherein said step of proffering an iris scan to an iris scan sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure.

[c35]   A method for facilitating biometric security in a smart-card transaction system comprising:
detecting a proffered iris scan at a sensor communicating with said system to obtain a proffered iris scan sample;
verifying the proffered iris scan sample; and
authorizing a transaction to proceed upon verification of the proffered iris scan sample.

[c36]   The method of claim 35, wherein said step of detecting further includes detecting a proffered iris scan at a sensor configured to communicate with said system via at least one of a smartcard, reader, and network.

[c37]   The method of claim 35, wherein said step of detecting a

proffered iris scan includes detecting a proffered iris scan at one of a video camera, an optical scanner, a digital camera, and a charge coupled device.

[c38]   The method of claim 35, wherein said step of detecting includes at least one of: detecting, storing, and processing a proffered iris scan sample.

[c39]   The method of claim 35, wherein said step of detecting further includes receiving a finite number of proffered iris scan samples during a transaction.

[c40]   The method of claim 35, wherein said step of detecting further includes logging each proffered iris scan sample.

[c41]   The method of claim 35, wherein said step of detecting further includes at least one of detecting, processing and storing at least one second proffered iris scan sample.

[c42]   The method of claim 35, wherein said step of detecting further includes using said iris scan sensor to detect at least one of pupil dilation, eyeball pressure and body heat.

[c43]   The method of claim 35, wherein said step of verifying includes comparing a proffered iris scan sample with a stored iris scan sample.

[c44]   The method of claim 43, wherein said step of comparing

a proffered iris scan sample with a stored iris scan sample comprises storing, processing and comparing surface patterns.

[c45] The method of claim 43, wherein comparing a proffered iris scan sample with a stored iris scan sample includes comparing a proffered iris scan sample with at least one of a biometric sample of a criminal, a terrorist, and a cardmember.

[c46] The method of claim 35, wherein said step of verifying includes verifying a proffered iris scan sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

[c47] The method of claim 35, wherein said step of verifying includes verifying a proffered iris scan sample using one of a local CPU and a third-party security vendor.